stickapp password manager

Powered by: RoboForm Enterprise

Installation & Configuration Guide

This document is provided to guide you through the process of installing and configuring StickApp Password Manager when used on SafeStick's managed by SafeConsole..

Overview

StickApp Password Manager is one of a number or Security and Productivity apps available for SafeStick, managed by SafeConsole's Publisher Feature.

StickApp Password Manager - powered by RoboForm - gives users the freedom and flexibility to securely carry all their passwords, identity information and bookmarks for use on any Windows host computer - anywhere in the world.

StickApp Password Manager can auto-login a user to applications and websites, and can fill out forms automatically saving hours of repetitive typing. Users really will find this one of the applications they cannot do without.

A very strong "Password Generator" features is also included. Users can be advised to replace insecure passwords with long, complex strong passwords - which are hard to remember but which Password Manager can generate, store and retrieve with ease.

All personal Password Manager data is totally secure and encrypted in TWO ways. The SafeStick encrypts it in Hardware; it is then encrypted again in software automatically by the application to AES 256bit military standards.

An upgrade to a fully Active Directory Integrated Enterprise version - which brings true Single Sign On and Password Management to the Enterprise without any expensive customisation or integration - is available on request.

CRITICAL NOTE: You **MUST** have followed the "StickApps Technical Installation Guide" which walks you through configuring SafeConsole and enabling the Publisher and Autostart features. **You absolutely must do this** before any StickApp will run on SafeSticks. If you have not done so please do this before proceeding with this document.

StickApp Password Manager System Requirements

- Microsoft Windows XP, Vista, 2003, 2008 or Windows 7.
- Approximately 12Mb available space on users SafeStick.

Licence

A trial licence for StickApp Password Manager is installed automatically, which allows a test number of logins (10), and a single identity per user to be created and saved.

For continued licenced use you must purchase a subscription. All licenced applications are fully supported.

An upgrade to the Active Directory Integrated version of Roboform Enterprise is also available on request.

Installation & Configuring

1. Extract the StickApp Password Manager download package to your desktop or other temporary location – you will have two root folders, one with the installation files, and one called Documentation. Copy / move the \passwordmanager folder to your own SafeConsole Publisher location – for example \\myserver\publisher\passwordmanager

   NOTE: In the Publisher UNC share you must now have a folder \passwordmanager which contains all of the sub-folders, programs, settings and other necessary associated files – approx 12Mb.

2. **CRITICAL STEP:** The Password Manager program utilises a very specific path for users data.

   <safestick root>\My Roboform Data\Default Profile

   This folder must be created on users SafeSticks, and populated with the supplied "Empty" Default Profile else the program simply will not run. You **MUST** configure the Autostart script file to do this automatically – see below for details.

   Having the users Data stored in this very specific location has two major benefits;

   a) User data will always be persistent, as it will always be stored in the personal storage area of their SafeStick. Even if Publisher is disabled, users saved data will always remain.

   b) If you have SafeConsole backup configured, personal user data will be automatically backed up to SafeConsole.

3. The "Default Profile" (which contains the recommended default settings for all of your SafeStick users) has been created for you as part of this package. If you wish to modify the settings in this Default Profile, it is necessary to check and set these settings before rolling out the solution. See further in this document for details on modifying this default profile.

Configuring AutoStart

NOTE: Follow the StickApps Technical Guide for creating and enabling Autostart in SafeConsole.

To Autostart StickApp Password Manager specifically;

1. In Windows Explorer, navigate to your Published UNC share where the Autostart.bat file is located - for example;

\\myserver\publisher\autostart

2. With Notepad or similar edit the Autostart.bat file

3. Add the following entry into the Autostart.bat file – for example;

```
>>
Echo Starting Password Manager......

REM First create and populate default empty data profile for PasswordManager if one doesnt exist..

if not exist %1"My Roboform Data" xcopy %1Applications\PasswordManager\Empty_Roboform_Data\"Default Profile"
%1"My Roboform Data\Default Profile" /D /S /E /C /I /Y

%1Applications\PasswordManager\Roboform\RoboForm.exe

exit
>>
```

NOTE: This xcopy statement in the Autostart file creates a new data folder if one does not exist, and populates it will the Default Settings. It then starts the program automatically. Edit this behaviour as required.

4. Save the file – making sure it is just called "autostart.bat" and not "autostart.bat.TXT"

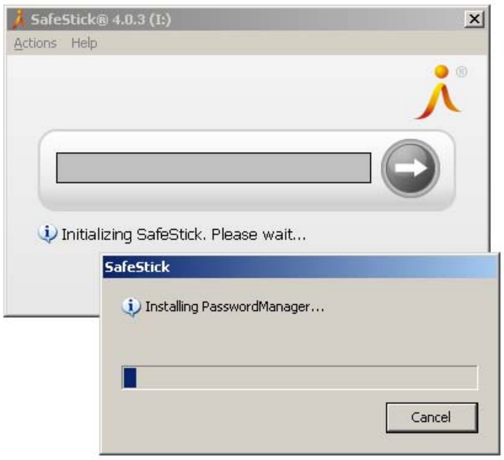
The next time a user in this OU group unlocks their SafeStick, this new Autostart file will be pushed to their SafeStick, Password Manager will be installed and started.

NOTE: You can add multiple entries into the autostart.bat script file to do any number of things (for example you may already have entries in the Autostart file to start StickApp Anti-Virus).

Please consult other StickApp install guides, for specific documentation on additional switches, commands, sub-routines and other information which may be required to autostart them.

Installation Behaviour

The next time a SafeStick is unlocked by a user in the OU Group you have specified for Publisher, StickApp Password Manager will be downloaded onto their SafeStick into a sub-folder of the <safestick drive letter>\Applications folder, and it will be started automatically.



Initializing SafeStick. Please wait...

Installing PasswordManager...

To Modify the Default Data Profile Settings:

- Installation steps 1 and 2 must above have been completed, and Autostart must have been configured.
- The Administrator unlocks their SafeStick and Password Manager will start for the first time.
- Administrator rights clicks on the Password Manager system tray icon, selects "Options" and makes configuration changes – such as Password Generator strength, Default Language, Autofill settings or Encryption type. **DO NOT** create a new Identity at this stage otherwise it will be Published for all users!
- Exit the Program.
- Administrator copies the folders from <safestick root>\My Roboform Data\Default Profile and overwrites the Published files in \\myserver\publisher\passwordmanager\Empty_Roboform_Data\Default Profile

Hiding / Un-Hiding StickApp Password Manager from the Shortcut Menu

By default we have configured “StickApp Password Manager” NOT to appear in the users SafeStick ShortCut menu.

This default has been chosen as the application is started automatically, it need not appear as a shortcut for users to run again – as it should already be running in the system tray as a small green suitcase looking icon.

If required you can Un-Hide the shortcut icon;

In \\myserver\publisher\passwordmanager edit the file called “SafeStick.ini”

Change the “yes” value to “no”

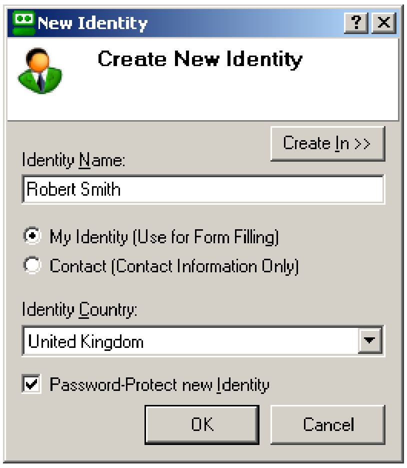
```
[starter]
hidden=no
```

The End User Interface – First Use Steps

Once installed an end user will notice a green suitcase looking icon down in the system tray by the clock.

On first use, a user should Right Click on the icon, and select “Identities”, then “New”.

- Enter your name.
- Select a “Master Password”. This is used to encrypt all of your Password Manager Data. **DO NOT FORGET IT** – it is one of two passwords (this one and your SafeStick password) that you need to remember!
- Populate your Identity card with as much or as little information as you like.
- Save and exit the Identity card.



Identity Name: Robert Smith

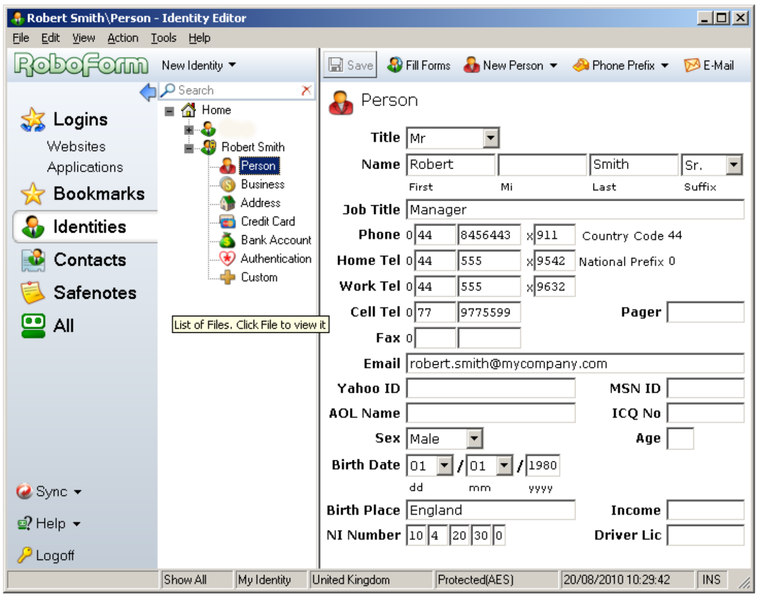
● My Identity (Use for Form Filling)

○ Contact (Contact Information Only)

Identity Country: United Kingdom

☑ Password-Protect new Identity

NOTE: In the trial version you can only save ONE Identity.



Title: Mr

Name: Robert | | Smith | Sr. (First, Mi, Last, Suffix)

Job Title: Manager

Phone: 0 44 8456443 x 911 Country Code 44

Home Tel: 0 44 555 x 9542 National Prefix 0

Work Tel: 0 44 555 x 9632

Cell Tel: 0 77 9775599 Pager

Fax: 0

Email: robert.smith@mycompany.com

Yahoo ID MSN ID

AOL Name ICQ No

Sex: Male Age

Birth Date: 01 / 01 / 1980 (dd mm yyyy)

Birth Place: England Income

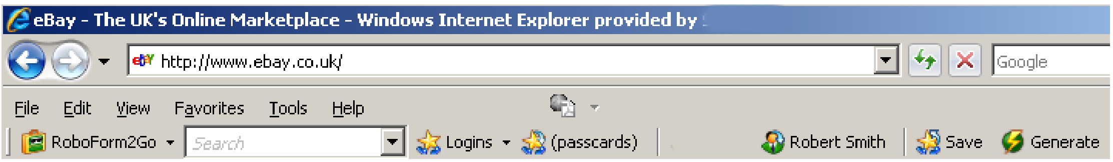
NI Number: 10 4 20 30 0 Driver Lic

Show All | My Identity | United Kingdom | Protected(AES) | 20/08/2010 10:29:42 | INS

Now whenever you start an Application or open a Browser to go to a Web page requiring login, or to fill a form which requires any user / address / other details, Password Manager will prompt you to save / fill your details.

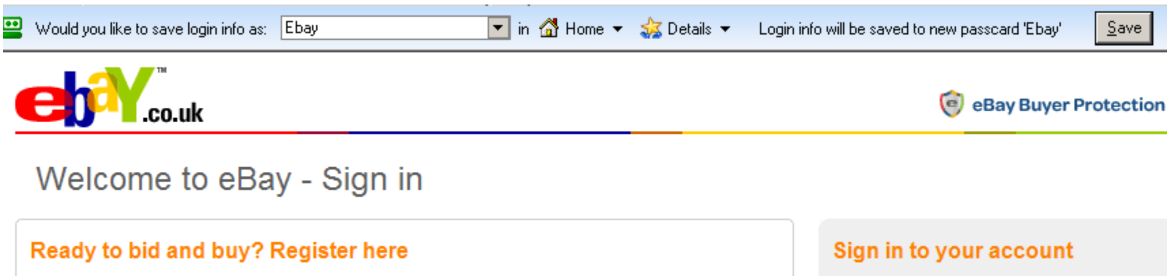
Testing Password Manager

- Start a Web browser such as Firefox or Internet Explorer. You will notice a new Password Manager toolbar has appeared and will contain the new Identity we created previously “Robert Smith”.


eBay - The UK's Online Marketplace - Windows Internet Explorer provided by

http://www.ebay.co.uk/

- Go to a website which requires your username and password – for example Ebay – Password Manager will ask if you wish to save your login details into a “PassCard” called Ebay (you can change the name if you like). Click Save.


Would you like to save login info as: Ebay in Home Details Login info will be saved to new passcard 'Ebay' Save

Welcome to eBay - Sign in

Ready to bid and buy? Register here

Sign in to your account

- Close the browser.
- Right click again on the icon near the clock, select Logins, you will see Ebay in the list. Simply select it and Password Manager will start the browser, take you to the website and will log you in automatically. This shortcut will also be available in the Browser toolbar, drop down box.

This procedure is virtually identical for Applications as well as Websites.

Additional Features

Additional Password Manager features such as Form Filling, SafeNotes and Strong Password Generator are not covered in this Installation guide. Please consult the user manual, context sensitive help in the program, or the online help.

Un-Installing StickApp Password Manager

StickApps are easily uninstalled – either individually or all installed StickApps completely - from users SafeSticks.

Option 1.

To remove ALL StickApps, start SafeConsole and disable the Publisher policy completely, or edit the Publisher policy from a selected OU Group as required.

The next time SafeSticks poll into SafeConsole to obtain policy, they will "know" that Publisher has been disabled and will delete all files from the <safestick driver letter>\Applications folder completely. Shortcuts will also be removed.

Option 2.

From your published share – for example \\myserver\publisher delete one or more StickApp folders as required. So to remove Password Manager simply delete entirely the \\myserver\publisher\passwordmanager folder.

NOTE: Removing StickApp Password Manager in this manner will NOT delete a persons saved Data.